International Journal on Semantic Web and Information Systems
Volume 20 • Issue 1

A Network Intrusion Detection Method for Information Systems Using Federated Learning and Improved Transformer

Qi Zhou, Guangdong Open University, China*
Zhoupu Wang, China Telecom Sichuan Branch, Chengdu, China

ABSTRACT

A network intrusion detection method for information systems using federated learning and improved transformer is proposed to address the problems of long detection time and low security and accuracy when analyzing massive data in most existing intrusion detection methods. Firstly, a network intrusion detection system is constructed based on a federated learning framework, and the transformer model is used as its universal detection model. Then, the dataset is divided and an improved generative adversarial network is used for data augmentation to generate a new sample set to overcome the influence of minority class samples. At the same time, the new samples are input into the transformer local model for network attack type detection and analysis. Finally, the authors aggregate the detection results of each local model and input them into the Softmax classifier to obtain the final classification prediction results.

KEYWORDS

Deep Learning, Federated Learning, Improve the Generation of Adversarial Networks, Network Intrusion Detection, Softmax Classifier, Transformer Model

1. INTRODUCTION

In the rapidly developing network environment, network security issues are constantly emerging. As an important measure to monitor potential network attacks, network intrusion detection (NID) needs to quickly and accurately identify attack events in a massive data environment (Vitorino, Praça, & Maia, 2023; Usoh, et al., 2023). Therefore, improving the accuracy and efficiency of network intrusion detection (NID) technology is of great practical significance (Krishna, et al. 2021).

Considering the complexity of network traffic and the development of computer technology, traditional ID methods have shortcomings in detecting attacks and have low detection efficiency (Wang, et al., 2023; Stergiou, et al., 2021; Devi, & Bharti, 2022). At present, various machine learning (ML) based NID methods have been proposed, and due to the ability of deep learning (DL) to learn complex patterns from high-dimensional data, it has become a suitable solution for detecting network attacks (Deore, & Bhosale, 2023; Mustafa, et al., 2023; Zhang, et al., 2023). ML and DL

DOI: 10.4018/IJSWIS.334845 *Corresponding Author

can be widely applied in ID, mainly due to the availability of collected network data, which can be used to train intrusion detection models. The development of technology has enhanced the computing power of devices, enabling faster training of data models while reducing costs, and the widespread application of DL ensures the accuracy of model optimization on the basis of self-learning. Although ML and DL have improved the detection accuracy, in reality, network intrusion data is limited and insufficient to train high-quality models with good performance (Yan, et al., 2023; Gaurav, et al. 2023). At the same time, there are still some issues with current intrusion detection methods: (1) users need to upload their data to a central entity to train the central model, but about 90% of the central entities will be attacked, resulting in poor security; (2) the performance of the system will decrease with the increase of user size, and single point of failure will be introduced, which will affect the integrity of services and the quality of the model; (3) traditional intrusion detection systems adopt a centralized processing mode, which is time-consuming and difficult to meet the current needs for fast and accurate detection.

The distributed machine learning framework - federated learning (FL), can effectively solve the above problems by implementing DL models in a distributed environment for training on datasets on different devices (Idrissi, et al., 2023; He, & Zhao, 2022). This can improve the efficiency of data feature extraction and learning while ensuring the privacy of terminal data for participants. To this end, a NID method for information systems is proposed based on FL and DL. The innovation of the proposed method is as follows:

1) To improve the processing efficiency and data security of massive data, the proposed method utilizes a FL framework for multi-server collaboration, which shortens training time.
2) Due to the small number of abnormal data samples, which directly affects the detection accuracy of the model, the proposed method utilizes an improved generative adversarial network for data augmentation to reduce the impact of minority class samples, while utilizing the Transformer model to ensure the reliability of detection.

2. RELATED RESEARCH

Traditional intrusion detection methods are based on fixed or dynamic rules to identify attacks on the network (Sawsan, et al., 2020). However, attackers use various techniques to disguise their attacks and disrupt the target's defense system (Xu, et al., 2021; Singh, & Gupta, 2022; Wang, et al., 2022). Therefore, ML algorithms were first widely used to detect anomalies in networks and have been proven to provide high detection rates. Supervised ML includes methods such as naive Bayesian classifiers (Ma., & Ding, 2022; Sharma, & Sharma, 2022). Supervised learning algorithms require classification and labeling of data, while unsupervised learning algorithms do not. Unsupervised algorithms include clustering, K-means, deep neural networks, etc. As shown in Zhang, & Wang, (2023), the use of feature engineering methods and synthetic minority class oversampling (SMOTE) technology to process network data can effectively reduce feature redundancy and alleviate the attack detection problem of class imbalance. At the same time, Catboos classifier is used to achieve network intrusion detection. Mohy, et al., (2023), propose a NID model for IoT environments based on KNN classifier and feature selection and utilize genetic algorithm for parameter optimization to ensure good detection performance. Maidamwar, et al., (2023), use a multi-layer perceptron classifier and a random forest algorithm to complete network intrusion detection. Layeghy, et al., (2023), propose using adversarial domains to extract domain invariant features from multiple network domains and apply unsupervised techniques for anomaly recognition, i.e. training One Class SVM (OSVM) models to detect network anomalies. The above methods, which rely solely on typical machine learning methods to construct intrusion detection methods, are no longer able to resist increasingly complex and diverse network threats. Therefore, there is a strong need for effective intrusion detection methods.